

Robust State Estimation against Sparse Integrity Attacks

Duo Han
School of EEE
Nanyang Technological
University
Singapore, 639798
dhanaa@ntu.edu.sg

Yilin Mo
School of EEE
Nanyang Technological
University
Singapore, 639798
ylmo@ntu.edu.sg

Lihua Xie
School of EEE
Nanyang Technological
University
Singapore, 639798
elhxie@ntu.edu.sg

ABSTRACT

We consider the problem of robust state estimation in the presence of integrity attacks. There are m sensors monitoring a dynamical process. Subject to the integrity attacks, p out of m measurements can be arbitrarily manipulated. The classical approach such as the MMSE estimation in the literature may not provide a reliable estimate under this so-called (p, m) -sparse attack. In this work, we propose a robust estimation framework where distributed local measurements are computed first and fused at the estimator based on a convex optimization problem. We show the sufficient and necessary conditions for robustness of the proposed estimator. The sufficient and necessary conditions are shown to be tight, with a trivial gap. We also present an upper bound on the damage an attacker can cause when the sufficient condition is satisfied. Simulation results are also given to illustrate the effectiveness of the estimator.

1. INTRODUCTION

Sensor networks have been increasingly applied in various cyber-physical systems (CPSs) such as smart grid [1] or Supervisory Control And Data Acquisition (SCADA) systems [2]. The sensors, however, are vulnerable to integrity attacks since in most cases they are spatially distributed and cannot be fully protected. Typically, the adversary can control a portion of all sensors and arbitrarily change their measurements during attacks. The objectives for launching such an attack in industrial systems may include using free electricity in smart grid, stealing resources like gasoline from oil caverns,

causing economical loss for rivals, etc. Two famous attacks on CPS hampering the critical infrastructure are Maroochy Water incident [3] and the first SCADA system malware (called Stuxnet) [4]. To sum up, Security in control and estimation systems has received much research attention [5].

In this article, we focus on the problem of robust state estimation based on compromised sensory data. The classical approach such as Kalman filtering cannot generate a reliable estimate in the presence of attacks. To put it simply, taking all measurements as important, e.g., (weighted) averaging all the measurements is not a good idea for robust estimation since one large measurement will drive the final estimate far deviated from the true value. To be concrete, we consider the problem of estimating the state $x \in \mathbb{R}^n$ of a dynamical process from measurements collected by m homogenous sensors, where the measurements are subject to Gaussian noise. Integrity attacks are very likely because the sensors cannot be fully protected due to practical reasons such as high maintenance cost. We assume the attacker can only take control of up to $p < m$ sensors since the resources of attacker may be limited and some sensors are physically untouchable. We put no restriction on what the attack is like. In other words, once a sensor is attacked, the sensory data can be arbitrarily manipulated.

Related Work: In the context of power systems, the estimation based on irregular sensor data has been formulated as bad data detection problem [6, 7]. A common practice is identifying the bad data or outliers by checking the corresponding residue. But this does not work well for intentional attacks [8–11]. For example, Liu et al. [8] showed that it is possible to launch a stealthy attack without being noticed. On the top of that, a so-called framing attack was studied in [11]. The detector is very likely to abandon the critical measurement under the framing attacks. Without the critical measurements, the network is unobservable and a stealthy attack is possible.

The robust estimator has been long studied in the field of statistics [12–19]. The robustness is often quan-

tified by breakdown points, e.g., the percentage of bad sensors, beyond which the estimate is unstable [20, 21]. However, the application of robustness analysis has not been extended to the estimation problem of a dynamical system yet.

For dynamical systems, compromised data detection via fault detection and isolation based methods has been extensively studied, [22–26]. However, in most of these works, the system is assumed to be noiseless, which greatly favors the failure detector. Pajic et al. [27] extended [25] by taking the bounded system noise into account. They proved that the worst error is still bounded for all possible attacks once the sufficient condition for exact data recovery in noiseless systems is satisfied. The drawback is that their approach is involved with zero-norm and thus computationally intractable, especially for large scale systems. In [28, 29], the authors studied the worst bias an attack can cause through reachability analysis and ellipsoid approximation.

The significance of this work is provide a robust estimation framework for estimating noisy systems compared with the noiseless case in [25]. To mitigate the damage injected by the attacker, we propose a robust estimator based on the convex optimization problem involving L_1 regulation which takes an advantage of analytical simplicity over [27]. The proposed estimator is shown to provide a robust estimate under some sufficient condition. Furthermore, the upper bound of the gap between the estimate without attacks and that under attacks is also quantified.

The rest of the paper is organized as follows. In Section 2 we formulate the robust estimation problem. We study the sufficient and necessary conditions for robustness in Section 3. We analyze the estimation performance in Section 4. Simulations are illustrated in Section 5. The concluding remarks are given in Section 6.

Notations: The i th entry of the vector u is denoted as $u[i]$. The L_p norm of the vector u is denote as $\|u\|_p$. If unspecified, $\|u\|$ means the L_2 norm of u by default. $\lfloor v \rfloor$ means the largest integer that is less than the scalar v .

2. PROBLEM SETUP

2.1 System Model

Assume that m homogenous sensors are measuring the following LTI system (see Fig. 1):

$$x(k+1) = Ax(k) + w(k). \quad (1)$$

The measurement equation for the i th sensor is given by

$$y_i(k) = Cx(k) + \varepsilon_i(k), \quad (2)$$

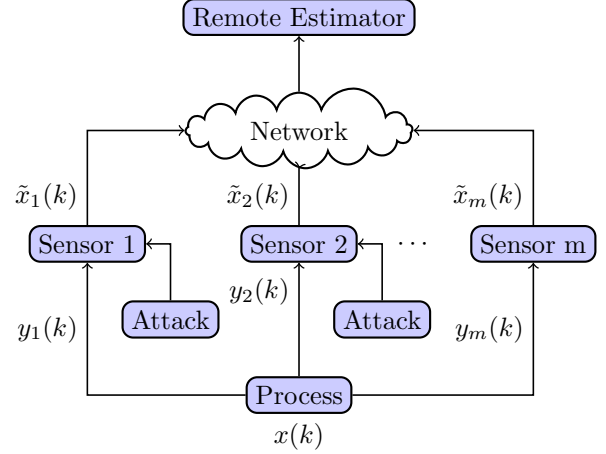


Figure 1: System Block Diagram.

where $x(k) \in \mathbb{R}^n$ is the state, $y_i(k) \in \mathbb{R}^l$ is the measurement collected by the i th sensor, $w(k) \in \mathbb{R}^n$ and $v(k) \in \mathbb{R}^l$ are the process noise and measurement noise for the i th sensor, respectively. The noise $w(k)$ and $\varepsilon_i(k)$'s are Gaussian distributed, *i.e.*,

$$w(k) \sim \mathcal{N}(0, Q), \quad \varepsilon_i(k) \sim \mathcal{N}(0, R).$$

The noises are assumed to be independent from each other across different time instants and sensors. Denote the tall measurement matrix $H \triangleq [C^\top, C^\top, \dots, C^\top]^\top \in \mathbb{R}^{lm \times n}$ and $y(k) \triangleq [y_1(k)^\top, y_2(k)^\top, \dots, y_m(k)^\top]^\top$. Denote $\Sigma = \text{diag}(R, \dots, R)$. The initial state $x(0)$ is Gaussian distributed with mean μ_0 and variance P_0 , and is independent from all noises. Assume that (A, C) is observable and $(A, Q^{\frac{1}{2}})$ is controllable.

Kalman filter is well known as the recursive minimum mean square error (MMSE) estimator:

$$\begin{aligned} \hat{x}_{KF}(k) &= (A - K(k)HA)\hat{x}_{KF}(k-1) + K(k)y(k), \\ P^-(k) &= AP(k-1)A^\top + Q, \\ P(k) &= (I_n - K(k)H)P^-(k), \end{aligned}$$

where the Kalman gain is given by

$$K(k) = P^-(k)H^\top(H P^-(k)H^\top + \Sigma)^{-1}. \quad (3)$$

The state error covariance $P^-(k)$ converges exponentially fast to \bar{P} which is obtained by solving the following discrete algebraic Riccati equation (DARE):

$$X = AXA^\top - AXH^\top(HXH^\top + \Sigma)^{-1}HXA^\top + Q. \quad (4)$$

Therefore, we assume the Kalman filter to be in the steady state, *i.e.*, $P(k) = (I_n - KH)\bar{P}$ and $K(k) = K$ from (3).

Due to the homogeneity of the sensors, we know that $K = [G, \dots, G]^\top$, $G \in \mathbb{R}^{n \times l}$. The Kalman filter

can be equivalently rewritten as:

$$\hat{x}_{KF}(k) = \frac{1}{m} \sum_{i \in \mathcal{S}} \tilde{x}_i(k), \quad (5)$$

where

$$\tilde{x}_i(k) = (A - KHA)\tilde{x}_i(k-1) + mGy_i(k), \quad (6)$$

This means the estimation process at the estimator can be decomposed into m sub-processes each of which only involves measurements from one sensor. This decomposition renders distributed estimation possible. To be specific, the sensor can locally compute $\tilde{x}_i(k)$ based on its own measurements and then the information fusion of all local estimates occurs at the remote estimator. It is worth noting that such distributed estimation is more resilient to attacks than the centralized estimation (all sensors transmit raw measurements). Since each local estimate of one sensor encodes all its historical measurements, corruption of one local estimate at some time instant causes little damage to the estimation.

Even if the sensor lacks computational capability and can only transmit raw measurements, each local estimation process can be computed at the central estimator. Therefore, without loss of generality, we assume each sensor computes a local estimate based on (6) and sends it to the estimator (see Fig. 1).

2.2 Attack Model

The attacker launches an integrity attack to the sensory data in different fashions. For example, it can change the physical environment to mislead the sensors or it hacks the onboard sensor chip or it can manipulate the data packet during the sensor-to-estimator transmission. No matter in which way the attack is launched, we have the following equation:

$$z_i(k) = \tilde{x}_i(k) + a_i(k), \quad (7)$$

where $z_i(k) \in \mathbb{R}^n$ is the “manipulated” local estimate and $a_i(k) \in \mathbb{R}^n$ is the attack vector. In other words, the attacker can change the local estimate of the i th sensor by $a_i(k)$. Define the local estimation error as $e_i(k) \triangleq x_k - \tilde{x}_i(k)$. Then we have

$$z_i(k) = x(k) + e_i(k) + a_i(k). \quad (8)$$

For concise notations, denote

$$\tilde{x}(k) \triangleq [\tilde{x}_1(k)^\top, \tilde{x}_2(k)^\top, \dots, \tilde{x}_m(k)^\top]^\top, \quad (9)$$

$$z(k) \triangleq [z_1(k)^\top, z_2(k)^\top, \dots, z_m(k)^\top]^\top, \quad (10)$$

$$e(k) \triangleq [e_1(k)^\top, e_2(k)^\top, \dots, e_m(k)^\top]^\top, \quad (11)$$

$$a(k) \triangleq [a_1(k)^\top, a_2(k)^\top, \dots, a_m(k)^\top]^\top.$$

Denote the index set of all sensors as $\mathcal{S} \triangleq \{1, 2, \dots, m\}$. For any index set $\mathcal{I} \subseteq \mathcal{S}$, define the complement set to be $\mathcal{I}^c \triangleq \mathcal{S} \setminus \mathcal{I}$. In our attack model, we assume that

the attacker can only compromise at most p sensors but can arbitrarily choose $a_i(k)$. The index set of malicious sensors is assumed to be time invariant. Formally, a (p, m) -sparse attack can be defined as

DEFINITION 1 ((p, m) -SPARSE ATTACK). *A vector a is called a (p, m) -sparse attack if there exists an index set $\mathcal{I} \subset \mathcal{S}$, such that:*

$$(i) \|a_i(k)\| = 0, \forall i \in \mathcal{I}^c;$$

$$(ii) |\mathcal{I}| \leq p.$$

Define the collection of a possible index set of malicious sensors as

$$\mathbb{C} \triangleq \{\mathcal{I} : \mathcal{I} \subset \mathcal{S}, |\mathcal{I}| = p\}.$$

The set of all possible (p, m) -sparse attacks is denoted as

$$\mathcal{A} = \mathcal{A}(k) \triangleq \bigcup_{\mathcal{I} \in \mathbb{C}} \{a(k) : \|a_i(k)\| = 0, i \in \mathcal{I}^c\}, \forall k.$$

After introducing the (p, m) -sparse attack, we need to formally define the robustness.

DEFINITION 2 (ROBUSTNESS). *An estimator*

$$g : \mathbb{R}^{mn} \mapsto \mathbb{R}^n$$

which maps the measurements $z(k)$ to a state estimate $\hat{x}(k)$ is said to be robust to the (p, m) -sparse attack if it satisfies the following condition:

$$\|g(\tilde{x}(k)) - g(\tilde{x}(k) + a(k))\| \leq \mu(\tilde{x}(k)), \forall a \in \mathcal{A}, \quad (12)$$

where $\mu : \mathbb{R}^{mn} \mapsto \mathbb{R}$ is a real-valued mapping on $\tilde{x}(k)$.

The robustness implies that the disturbance on the state estimate caused by an arbitrary attack is bounded. A trivial robust estimator is $g(y) = 0$ which provides a very poor estimate. Therefore, another desirable property for an estimator is translation invariance, which is defined as follows:

DEFINITION 3 (TRANSLATION INVARIANCE). *An estimator g is translation invariant if $g(z + Eu) = u + g(z)$, $\forall u \in \mathbb{R}^n$, where $E \triangleq [I_n, \dots, I_n]^\top$.*

REMARK 1. *Notice that if an estimator is robust and translation invariant, then*

$$\begin{aligned} & \|g(\tilde{x}(k)) - g(\tilde{x}(k) + a(k))\| \\ &= \|Ex(k) + g(e(k)) - Ex(k) + g(e(k) + a(k))\| \\ &= \|g(e(k)) - g(e(k) + a(k))\| \leq \mu(e(k)). \end{aligned}$$

Therefore, the maximum bias that can be injected by an adversary is only a function of the noise $e(k)$.

2.3 A Robust Estimator

Apparently, the linear estimator (5) cannot give an estimate with bounded error even when only one estimate is arbitrarily manipulated. In other words, there is a conflict between the MMSE optimality and the robustness against attacks.

The main task of this work is to design a robust estimator which achieves a desirable tradeoff between the MMSE optimality and the robustness, and investigate the sufficient and necessary conditions to be robust to (p, m) -sparse attacks. To this end, a general estimator is proposed as follows:

$$\hat{x}(k) \triangleq g(z(k)) = \arg \min_{\hat{x}(k)} \sum_{i \in S} \varphi(z_i(k) - \hat{x}(k)), \quad (13)$$

where $\varphi : \mathbb{R}^n \mapsto \mathbb{R}$. We notice that to recover Kalman filter we can choose φ to be L_2 norm. The candidate functions of φ may include L_p norm or LASSO [30], to just name a few.

Though there are many important estimators as special cases of (13), we mainly focus on the properties of the following concrete estimator in the rest of this paper. The same methodology can be extended to other φ 's. Pajic et al. [27] proposed the following robust estimator in the presence of integrity attack:

$$\begin{aligned} & \underset{\hat{x}(k), a, e(k)}{\text{minimize}} && \sum_{i \in S} \|e_i(k)\|_2^2 \\ & \text{subject to} && z_i(k) = \hat{x}(k) + e_i(k) + a_i(k), \forall i, \\ & && a \in \mathcal{A}. \end{aligned}$$

However, the minimization problem involves zero-norm, and thus is difficult to solve in general. A commonly adopted approach is to use L_1 relaxation to approximate zero-norm, which leads to the following minimization problem:

$$\begin{aligned} & \underset{\hat{x}(k), a, \varpi(k)}{\text{minimize}} && \sum_{i \in S} \|\varpi_i(k)\|_2^2 + \lambda \sum_{i \in S} \|a_i(k)\|_1 \\ & \text{subject to} && z_i(k) = \hat{x}(k) + \varpi_i(k) + a_i(k), \forall i. \end{aligned} \quad (14)$$

If we define the following function $F : \mathbb{R}^n \mapsto \mathbb{R}$:

$$F(u) \triangleq \underset{v \in \mathbb{R}^n}{\text{minimize}} \quad \|u - v\|_2^2 + \lambda \|v\|_1, \quad (15)$$

then one can easily prove that the optimization problem (14) can be rewritten as

$$\hat{x}(k) \triangleq g(z(k)) = \arg \min_{\hat{x}(k)} \sum_{i \in S} F(z_i(k) - \hat{x}(k)). \quad (16)$$

In the next section, we shall present sufficient and necessary conditions for the robustness of the estimator (16). For concise notation, we will omit the time index k if it is clear from the context.

3. ROBUST ANALYSIS

We provide an answer to the following question in this section: in what condition the proposed estimator in (16) satisfies the robustness requirement (12)?

Before preceding to the main results, we give an explicit form of $F(u)$ given in (15). We can decompose $F(u)$ by letting $F(u) = \sum_{i=1}^n f(u_i)$, where u_i is the i th entry of u and $f(\tau) : \mathbb{R} \mapsto \mathbb{R}$ is given by

$$f(\tau) \triangleq \underset{v \in \mathbb{R}}{\text{minimize}} \quad (\tau - v)^2 + \lambda |v|, \quad (17)$$

We define the RHS of (17) as

$$\pi(v) \triangleq (\tau - v)^2 + \lambda |v|.$$

Applying the KKT conditions, we know that

$$0 \in \partial \pi(a^*) = -2\tau + 2v^* + \text{sgn}(v)\lambda.$$

Since $\pi(v)$ is not differentiable at $v = 0$, by calculating the subgradient we have that

$$v^* = 0, \text{ if } |\tau| \leq \frac{\lambda}{2}.$$

For $v^* \neq 0$, by letting

$$0 = -2\tau + 2v^* + \text{sgn}(v^*)\lambda,$$

we obtain that

$$v^* = \begin{cases} \tau - \frac{\lambda}{2}, & \text{if } \tau > \frac{\lambda}{2}, \\ \tau + \frac{\lambda}{2}, & \text{if } \tau < -\frac{\lambda}{2}. \end{cases}$$

Therefore, we have f explicitly written as:

$$f(\tau) = \begin{cases} \tau^2, & \text{if } |\tau| \leq \frac{\lambda}{2}, \\ \lambda |\tau| - \frac{\lambda^2}{4}, & \text{if } |\tau| > \frac{\lambda}{2}. \end{cases} \quad (18)$$

In the next proposition we present some useful properties of f and F .

PROPOSITION 1. *The properties of f and F are summarized as follows:*

- (i) f and F are convex.
- (ii) f and F are symmetric, i.e., $f(u) = f(-u)$.
- (iii) f and F are non-negative and $f(0) = 0$.
- (iv) f and F are twice differentiable.

The results are easy to verify and omitted here.

To obtain the sufficient and necessary conditions for robustness, we first need to show some findings on the derivative of F . To facilitate the analysis, we define two functions. For all $u, v \in \mathbb{R}^n$ and $t \in \mathbb{R}$, define $h : \mathbb{R}^n \times \mathbb{R}^n \times \mathbb{R} \mapsto \mathbb{R}$ as follows:

$$h(u, v, t) \triangleq F(v + tu).$$

Define the mapping $\phi : \mathbb{R}^n \mapsto \mathbb{R}^n$,

$$\phi(u) \triangleq \nabla F(u) = [\nabla f(u[1]), \dots, \nabla f(u[n])]^\top, \quad (19)$$

where

$$\nabla f(u[i]) = \begin{cases} 2|u[i]|, & \text{if } |u[i]| \leq \frac{\lambda}{2}, \\ \text{sgn}(u[i])\lambda, & \text{if } |u[i]| > \frac{\lambda}{2}, \end{cases} \quad (20)$$

where $\text{sgn}(\cdot)$ is defined as: if $s = \text{sgn}(v)$, then

$$s[i] = \begin{cases} +1, & \text{if } v[i] \geq 0, \\ -1, & \text{if } v[i] < 0. \end{cases}$$

Notice that a useful equality in the sequel is

$$\frac{\partial h(u, v, t)}{\partial t} = \phi(v + tu)^\top u.$$

LEMMA 1. *The following statements are true:*

(i) *The limit below is well defined for all $u \in \{u \in \mathbb{R}^n : \|u\| < \infty\}$, i.e.,*

$$C(u) \triangleq \lim_{t \rightarrow \infty} \frac{\partial h(u, 0, t)}{\partial t} = \lambda \|u\|_1, \quad (21)$$

(ii) *The following pointwise limit holds:*

$$\lim_{t \rightarrow \infty} \frac{\partial h(u, v, t)}{\partial t} = C(u). \quad (22)$$

Moreover, the convergence is uniform on any compact set of (u, v) .

(iii) *For any u, v , we have that*

$$\phi(v + u)^\top u \leq C(u). \quad (23)$$

PROOF. (i) It is easy to see that

$$\begin{aligned} & \lim_{t \rightarrow \infty} \frac{\partial h(u, 0, t)}{\partial t} \\ &= \lim_{t \rightarrow \infty} \phi(tu)^\top u = \lambda \sum_{i=1}^n \text{sgn}(u[i])u[i] = \lambda \|u\|_1. \end{aligned}$$

(ii) We have that

$$\lim_{t \rightarrow \infty} \frac{\partial h(u, v, t)}{\partial t} = \lim_{t \rightarrow \infty} \phi(v + tu)^\top u = \lambda \|u\|_1.$$

Due to the convexity of F , $\partial h(u, v, t)/\partial t$ is monotonically non-decreasing with respect to t . Furthermore, $C(u)$ is continuous since it is a norm. Therefore, by Dini's theorem [31], $\partial h(u, v, t)/\partial t$ converges uniformly to $C(u)$ on a compact set of (u, v) .

(iii) From (19), we know that

$$\phi(v + u)^\top u \leq \sum_{i=1}^n \lambda u[i] \leq \lambda \|u\|_1.$$

Therefore, we conclude that $\phi(v + u)^\top u \leq C(u)$ for any u, v .

□

REMARK 2. *Intuitively speaking, one can interpret F as a potential field and the derivative of F as the force generated by each sensor. By (23), we know that the force from the potential field F along the u direction cannot exceed $C(u)$. On the other hand, Equation (22) implies that this bound is achievable.*

We are now ready to give the sufficient condition for the robustness of the estimator.

THEOREM 1 (SUFFICIENT CONDITION). *If the following conditions hold:*

$$2p < m, \quad (24)$$

then the estimator g is robust.

PROOF. Our goal is to prove that there exists a $\beta(\tilde{x})$, such that for any $t > \beta(\tilde{x})$, $\|u\| = 1$, $a \in \mathcal{A}$, the following inequality holds:

$$\sum_{i \in \mathcal{S}} \frac{\partial h(-u, z_i, t)}{\partial t} > 0. \quad (25)$$

As a result, any point $\|\hat{x}\| > \beta(\tilde{x})$ cannot be the solution of the optimization problem since there exists $\epsilon > 0$ such that $(\|\hat{x}\| - \epsilon)\hat{x}/\|\hat{x}\|$ is a better point. Therefore, we must have $\|g(z)\| \leq \beta(\tilde{x})$ and hence the estimator is robust.

To prove (25), we will first look at benign sensors. We can always find a finite constant N_i depending on δ and \tilde{x}_i such that for all $t \geq N_i(\delta, \tilde{x}_i)$, the following inequality holds:

$$\frac{\partial h(-u, z_i, t)}{\partial t} \geq C(u) - \delta = \lambda - \delta, \quad (26)$$

for any $\|u\| = 1$. We define $\beta(z) \triangleq \max_{1 \leq i \leq m} N_i(\delta, \tilde{x}_i)$ and fix δ to be

$$\delta = \frac{(m - 2p)\lambda}{m}. \quad (27)$$

Hence, for $i = 1, \dots, m$, if $t > \beta_\delta(z)$ we know that

$$\sum_{i \in \mathcal{I}^c} \frac{\partial h(-u, z_i, t)}{\partial t} \geq (m - p)(\lambda - \delta), \quad \forall \|u\| = 1. \quad (28)$$

We now consider malicious sensors. By Lemma 1 (iii), we know that for $i \in \mathcal{I}$, and any u

$$\begin{aligned} \phi(z_i - tu)^\top tu &= \phi(z_i - 2tu + tu)^\top tu \leq C(tu) \\ \Rightarrow \phi(z_i - tu)^\top u &\geq -\lambda. \end{aligned}$$

Then we have

$$\sum_{i \in \mathcal{I}} \frac{\partial h(-u, z_i, t)}{\partial t} \geq -p\lambda, \quad \forall \|u\| = 1. \quad (29)$$

Hence from (27), (29) and (28), we know that

$$\sum_{i \in \mathcal{S}} \frac{\partial h(-u, z_i, t)}{\partial t} \geq (m - p)(\lambda - \delta) - p\lambda > 0,$$

which proves (25). \square

It is shown that if the number of malicious sensors is less than the good sensors, then the estimator is robust. The intuition is that the sum force injected by any p sensors from the potential field F along the u direction must be able to be balanced by the sum force of the rest $m - p$ sensors, *i.e.*, zero-sum. Otherwise, the optimal estimate must lie in the infinity due to unbalanced driving forces along u and thus violates the robustness defined in (12).

We next present a necessary condition for the robustness of the estimator.

THEOREM 2 (NECESSARY CONDITION). *If the following condition is satisfied:*

$$2p > m,$$

then the estimator is not robust to the attack.

PROOF. The robustness of the estimator is equivalent to that the optimal estimate \hat{x} satisfies $\|\hat{x}\| \leq \mu(z)$ for all $a \in \mathcal{A}$, where μ is a real-valued function. To this end, we will prove that for any $r > 0$, there exists a y such that all \hat{x} that satisfies $\|\hat{x}\| \leq r$ cannot be the optimal solution of (16).

We will first look at the compromised sensors. For every $\delta > 0$ we can always find a finite constant $N_i(\delta)$ such that for any $\hat{x} \in \{\hat{x} : \|\hat{x}\| \leq r\}$ and for all $t > N_i$, the following inequality holds:

$$\frac{\partial h(u, z_i - \hat{x}, t)}{\partial t} \geq C(u) - \delta \quad (30)$$

The inequality is due to the uniform convergence of $h(u, v, t)$ to $C(u)$ on $\{u\} \times \{v : v = z_i - \hat{x}, \|x\| \leq r\}$.

Let us choose

$$\delta = \frac{2p - m}{m} C(u),$$

and $t = \max_{i \in \mathcal{I}} N_i(\delta)$ and $z_i = tu$ for all $i \in \mathcal{I}$, then we know for any $\|\hat{x}\| \leq r$,

$$\sum_{i \in \mathcal{I}} \frac{\partial h(u, z_i - \hat{x}, t)}{\partial t} \geq pC(u) - p\delta.$$

Now let us look at the benign sensors. By Lemma 1 (iii) we have

$$\frac{\partial h(u, \tilde{x}_i - \hat{x}, t)}{\partial t} \geq -C(u). \quad (31)$$

From (30) and (31),

$$\sum_{i \in \mathcal{S}} \frac{\partial h(u, z_i - \hat{x}, t)}{\partial t} \geq (m - p)C(u) - pC(u) + p\delta > 0$$

Thus for such a z_i satisfying

$$y_i = \begin{cases} \tilde{x}_i, & \text{if } i \in \mathcal{I}^c \\ tu, & \text{if } i \in \mathcal{I}, \end{cases}$$

$\hat{x} + u$ is a better estimate than all \hat{x} satisfying $\|\hat{x}\| \leq r$. Since r is an arbitrary positive real number, we can conclude that the estimator is not robust. \square

4. PERFORMANCE ANALYSIS

In the previous section we have studied the robustness of the estimator. Now we focus our attention on the performance of the proposed estimator. We concern two questions in this section. The first one is the sufficient condition that the estimator gives an MMSE estimate when there is no attack. The other one is what is the maximum damage that an attacker can cause to the estimate, *i.e.*, the upper bound of $\|g(\tilde{x}(k)) - g(\tilde{x}(k) + a(k))\|$.

4.1 Without attacks

When no attacks are present, an MMSE estimate like a Kalman filter provides is still preferred. Notice that the proposed robust estimator indeed probabilistically provides an MMSE estimate. A sufficient condition for providing the MMSE estimate \hat{x}_{KF} given in (5) is given as follows.

LEMMA 2. *If $\tilde{x} \in \mathcal{G}$, where*

$$\mathcal{G} \triangleq \{\tilde{x} \in \mathbb{R}^{mn} : \max_{i \in \mathcal{S}} \|\tilde{x}_i - \hat{x}_{KF}\|_1 \leq \frac{\lambda}{2}\}, \quad (32)$$

then $\hat{x} = \hat{x}_{KF}$.

PROOF. From (32) and (18), we know that \hat{x}_{LS} is a solution of (16). \square

Now we characterize the pdf of \tilde{x} . Define the local estimation error covariance of the i th sensor and the local cross estimation error covariance between the i th sensor and the j th sensor as

$$P_{ii}(k) \triangleq \mathbb{E}[e_i(k)e_i(k)^\top | y_i(1), \dots, y_i(k)],$$

$$P_{ij}(k) \triangleq \mathbb{E}[e_i(k)e_j(k)^\top | y_i(1), y_j(1), \dots, y_j(k), y_j(k)].$$

From (6), the error dynamics of the i th sensor estimate is thus given as follows:

$$e_i(k) = (A - KHA)e_i(k-1) + (mGC - I_n)w(k) + mG\varepsilon_i(k). \quad (33)$$

Note that the local estimator for each sensor is a stable estimator since the spectral radius of $A - KHA$ is less than one [32]. It is easy to see that $P_{ii}(k)$ converges to \bar{P}_{ii} at the steady state, where \bar{P}_{ii} is the unique solution of the following Lyapunov equation of X :

$$X = (A - KHA)X(A - KHA)^\top + (mGC - I_n)Q(mGC - I_n)^\top + m^2GRG^\top. \quad (34)$$

Similarly, $P_{ij}(k)$ converges to \bar{P}_{ij} , where \bar{P}_{ij} is the unique solution of the following Lyapunov equation of

X :

$$X = (A - KHA)X(A - KHA)^\top + (mGC - I_n)Q(mGC - I_n)^\top. \quad (35)$$

Denote $\Gamma = \{\bar{P}_{ij}\} \in \mathbb{R}^{nm \times nm}$. Now we know the probability density function of \tilde{x} , *i.e.*,

$$\tilde{x} \sim \mathcal{N}(x, \Gamma),$$

and thus the distribution of \hat{x}_{KF} . We can compute the probability of generating the MMSE estimate

$$\Pr(\tilde{x} \in \mathcal{G}) = \int_{x \in \mathcal{G}} \mathcal{N}(x, \Gamma) d\tilde{x}. \quad (36)$$

The integration is not trivial and numerical methods can be used to approximate $\Pr(\tilde{x} \in \mathcal{G})$. A closed-form solution to $\Pr(\tilde{x} \in \mathcal{G})$ is left as an open question.

Another interesting observation is that the larger λ is, the more likely the MMSE estimate is.

4.2 Under attacks

We now consider the worst damage that an attacker can cause, *i.e.*, the maximum deviation between the estimate under attacks and that without attacks. If the necessary condition in Theorem 2 is violated, the estimator is not robust and thus the deviation can be arbitrarily large. A more interesting question is how to obtain $\mu(\tilde{x})$ in (12) for all possible attacks if the estimator is robust.

Suppose the sufficient condition in Theorem 1 is satisfied. Let the robust estimate without attacks to be $\hat{x}_R = g(\tilde{x})$. Due to the translation invariance, we have

$$\begin{aligned} \|g(\tilde{x}) - g(\tilde{x} + a)\|_1 \\ = \|\hat{x}_R - g(\tilde{x} + a)\|_1 = \|g(z - E\hat{x}_R)\|_1 \leq \mu(\tilde{x}). \end{aligned}$$

Denote $\tilde{z}_i \triangleq z_i - \hat{x}_R$, $\tilde{z} = [\tilde{z}_1, \dots, \tilde{z}_m]$, and $\tilde{x}_i \triangleq \tilde{x}_i - \hat{x}_R$, $\tilde{x} = [\tilde{x}_1, \dots, \tilde{x}_m]$.

Similar to the proof of Theorem 1, there exists β^* such that for any $\beta \in \{\beta : \|\beta\|_1 > \|\beta^*\|_1\}$ the following inequality holds:

$$\sum_{i \in \mathcal{S}} \phi(\tilde{z}_i - \beta)^\top \text{sgn}(\beta) > 0 \quad (37)$$

In other words, we want to find a β^* such that

$$\sum_{j=1}^n \sum_{i \in \mathcal{S}} \nabla f(\tilde{z}_i[j] - \beta^*[j]) \text{sgn}(\beta^*[j]) = 0, \quad \forall j = 1, \dots, n, \quad (38)$$

where $\tilde{z}_i[j]$ and $\beta^*[j]$ are the j th entry of \tilde{z}_i and β^* respectively.

Define the two mapping $\underline{\kappa}, \bar{\kappa} : \mathbb{R}^m \times \mathbb{R} \times \mathbb{R} \mapsto \mathbb{R}$ for

any vector u and scalars p, m :

$$\begin{aligned} \underline{\kappa}(u, p, m) &\triangleq \left\{ u[i] : |\{u[j] : u[j] \leq u[i], j \neq i\}| = \left\lfloor \frac{m-2p}{2} \right\rfloor + 1 \right\}, \\ \bar{\kappa}(u, p, m) &\triangleq \left\{ u[i] : |\{u[j] : u[j] \geq u[i], j \neq i\}| = \left\lfloor \frac{m-2p}{2} \right\rfloor + 1 \right\}. \end{aligned}$$

Let $\zeta_j \triangleq [\check{x}_1[j], \dots, \check{x}_m[j]]^\top$. Then we denote $(\underline{\theta}_j, \bar{\theta}_j)$ to be

$$(\underline{\theta}_j, \bar{\theta}_j) = (\underline{\kappa}(\zeta_j, p, m), \bar{\kappa}(\zeta_j, p, m)), \quad j = 1, \dots, n. \quad (39)$$

Now we are ready to present the upper bound on the worst damage.

THEOREM 3. *The upper bound $\mu(\tilde{x})$ is shown as follows :*

$$\mu(\tilde{x}) = \|\beta^+\|_1, \quad (40)$$

where $\beta_j^+ = \max(|\underline{\theta}_j - \lambda/2|, |\bar{\theta}_j + \lambda/2|)$, $i = 1, \dots, n$.

PROOF. A sufficient condition for (38) is that for each j the following inequality holds:

$$\sum_{i \in \mathcal{S}} \nabla f(\tilde{z}_i[j] - \beta[j]) \text{sgn}(\beta^*[j]) = 0. \quad (41)$$

We first show that $\beta^*[j]$ must lie in $[\underline{\theta}_j - \lambda/2, \bar{\theta}_j + \lambda/2]$. We prove this by contradiction. Suppose $\beta^*[j] < \underline{\theta}_j - \lambda/2$. For any possible \mathcal{I}^c , we then have

$$\sum_{i \in \mathcal{I}^c} \nabla f(\tilde{z}_i[j] - \beta[j]) \text{sgn}(\beta^*[j]) \geq (m-p)\lambda.$$

This is due to the facts that there are at least $m-p$ points of $\tilde{z}_i[j]$ are $\lambda/2$ larger than $\beta^*[j]$ from (39) and that the maximum gradient is λ from (20).

On the other hand, from Lemma 1 (iii) we know that for any possible \mathcal{I} ,

$$\left| \sum_{i \in \mathcal{I}} \nabla f(\tilde{z}_i[j] - \beta[j]) \text{sgn}(\beta^*[j]) \right| \leq p\lambda.$$

Hence (41) cannot hold for $\beta^*[j] < \underline{\theta}_j - \lambda/2$. Similar arguments applies for $\beta^*[j] > \bar{\theta}_j + \lambda/2$. Therefore, we know that $\beta^*[j] \in [\underline{\theta}_j - \lambda/2, \bar{\theta}_j + \lambda/2]$. If we take the maximum over $(|\underline{\theta}_j - \lambda/2|, |\bar{\theta}_j + \lambda/2|)$ as $\beta^+[j]$, then any β satisfying $\|\beta\|_1 > \|\beta^+\|_1$ cannot be $g(z - E\hat{x}_R)$. \square

5. SIMULATION RESULTS

In this section we illustrate the main results using numerical examples.

Consider a linear system with

$$A = \begin{bmatrix} 0.95 & 1 \\ 0 & 1.01 \end{bmatrix}, Q = \begin{bmatrix} 1.5 & 1 \\ 1 & 2 \end{bmatrix}$$

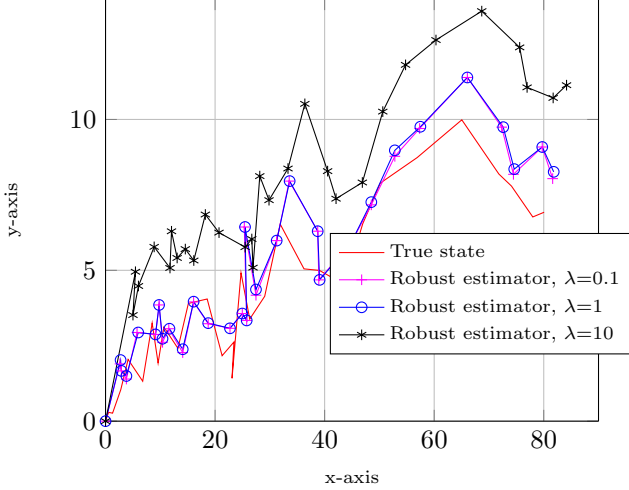


Figure 2: Trajectory of the system state and robust estimate with different λ . The number of malicious sensors is 2 out of 5. When $p > m/2$, the estimate goes unbounded. The robust estimator with $\lambda = 10$ performs worst.

is monitored by $m = 5$ sensors with

$$C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, R = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}.$$

First we verify the sufficient and necessary conditions for robustness. Assume the number of the malicious sensor is $p = 2$. In Fig. 2 we depict the trajectory of the true state and show that the proposed robust estimators give reliable estimates with bounded error. As comparison, we also plot the case when there are no attacks in presence in Fig. 3. Still all the estimators compute reliable estimates. Notice that the estimator with $\lambda = 10$ resembles the Kalman filter most. This collides with the intuition that a large penalty parameter λ performs poorly in Fig. 2 but works well without attacks.

In Table. 5 we show the relationship between the penalty parameter λ and the probability of recovering Kalman filter when there is no attack. On the other hand, we plot the upper bound $\mu(\tilde{x})$ given in Theorem 3 and the true gap $\|g(\tilde{x}) - g(z)\|_1$ versus time. Notice that when $\lambda = 1$ or $\lambda = 0.1$, the upper bound on the deviation caused by attacks is smaller. In other words, the estimator is more robust with a small λ . Tradeoff between robustness when the sensors are under attack and the MMSE optimality when the attacker is not present is clearly shown via different λ 's.

6. CONCLUDING REMARKS

In this work we have studied the robust state estimation problem in the presence of integrity attacks. The

λ	1	2	5	10
$\Pr(\hat{x} = \hat{x}_{KF})$	0.0001	0.013	0.48	0.98

Table 1: Relationship between the penalty parameter λ and the probability of recovering Kalman filter when there is no attack.

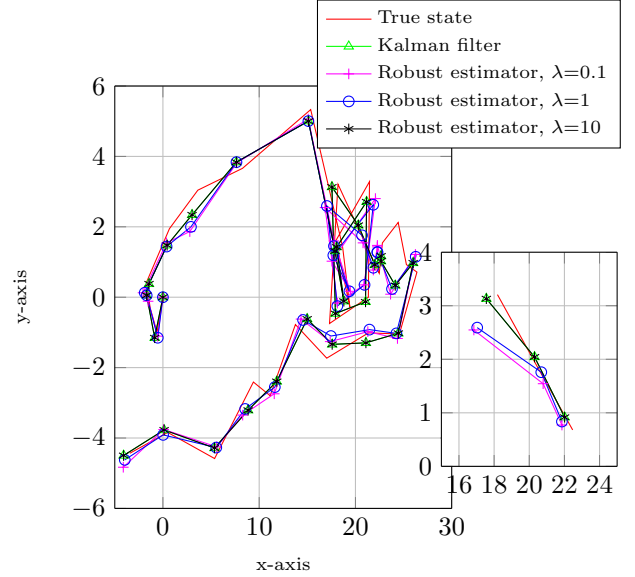


Figure 3: Trajectory of the system state and robust estimate with different λ without attacks. The robust estimator with $\lambda = 10$ resembles the Kalman filter most.

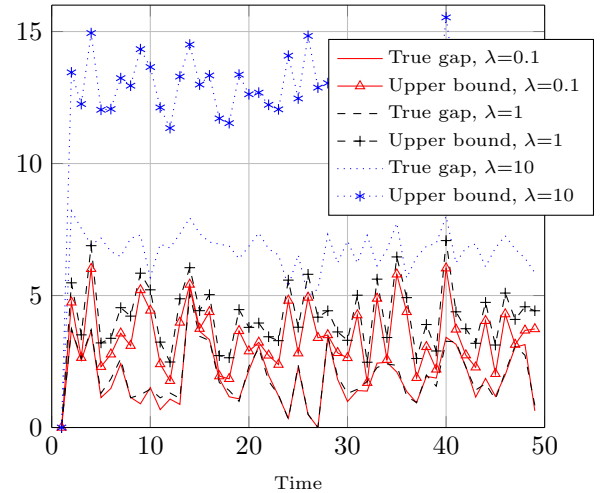


Figure 4: Upper bound $\mu(\tilde{x})$ and the true gap versus time. The number of malicious sensors is 2 out of 5. The robust estimator with $\lambda = 10$ has the largest upper bound and the true gap.

attacker can control p out of m sensors and can arbitrarily change the measurement. We have proposed a robust estimation framework and formulated a convex optimization problem with L_1 regulation to find the robust estimate. We have also shown the sufficient and necessary conditions for the estimator is robust against the (p, m) -sparse attack. Informally speaking, the percentage of compromised sensors should be less than a half to guarantee the robustness. Furthermore, we have analyzed the estimation performance without attacks and under attacks. Further work includes the robust estimation with inhomogeneous sensors.

7. REFERENCES

- [1] S. Massoud Amin and B. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *IEEE Power and Energy Mag.*, vol. 3, no. 5, pp. 34–41, Sep. 2005.
- [2] S. A. Boyer, "SCADA: supervisory control and data acquisition," *Instrument Engineers' Handbook, Volume Three: Process Software and Digital Networks*, p. 357, 2002.
- [3] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," *Critical Infrastructure Protection*, p. 73.
- [4] T. M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.
- [5] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proc. Conf. Hot Topics in Security*. Berkeley, CA, USA: USENIX Association, 2008, pp. 1–6.
- [6] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Trans. Power Apparatus and Systems*, vol. 94, no. 2, pp. 329–337, Mar. 1975.
- [7] L. Mili, T. Van Cutsem, and M. Ribbens-Pavella, "Bad data identification methods in power system state estimation - a comparative study," *IEEE Power Engineering Review*, vol. PER-5, no. 11, pp. 27–28, Nov. 1985.
- [8] Y. Liu, M. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conf. Computer and Commun. Security*, 2009.
- [9] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *First Workshop on Secure Control Systems*, 2010.
- [10] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, 2011.
- [11] J. Kim, L. Tong, and R. J. Thomas, "Data framing attack on state estimation," *IEEE J. Selected Areas in Commun.*, vol. 32, no. 7, pp. 1460–1470, Jul. 2014.
- [12] F. R. Hampel, "The influence curve and its role in robust estimation," *J. the American Statistical Association*, vol. 69, no. 346, pp. 383–393, 1974.
- [13] S. Kassam, H. V. Poor *et al.*, "Robust techniques for signal processing: A survey," *Proc. IEEE*, vol. 73, no. 3, pp. 433–481, 1985.
- [14] R. A. Maronna, D. R. Martin, and V. J. Yohai, *Robust Statistics: Theory and Methods*. NJ: Wiley, 2006.
- [15] P. J. Huber and E. M. Ronchetti, *Robust Statistics*. NJ: Wiley, 2009.
- [16] V. J. Yohai and R. H. Zamar, "High breakdown-point estimates of regression by means of the minimization of an efficient scale," *J. the American Statistical Association*, 2012.
- [17] P. Rousseeuw and C. Croux, "Explicit scale estimators with high breakdown point," 1992.
- [18] O. Hössjer, "Rank-based estimates in the linear model with high breakdown point," *J. the American Statistical Association*, vol. 89, no. 425, pp. 149–158, 1994.
- [19] P. J. Rousseeuw, "Least median of squares regression," *J. the American Statistical Association*, 2012.
- [20] F. R. Hampel, "A general qualitative definition of robustness," *The Annals of Mathematical Statistics*, vol. 42, no. 6, pp. 1887–1896, 1971.
- [21] D. L. Donoho and P. J. Huber, "The notion of breakdown point," *A Festschrift for Erich L. Lehmann*, pp. 157–184, 1983.
- [22] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: a system theoretic approach," *IEEE Transactions on Automatic Control*, vol. 57, no. 1, pp. 90–104, Jan 2010.
- [23] F. Pasqualetti, F. Dorfler, and F. Bullo, "Cyber-physical attacks in power networks: models, fundamental limitations and monitor design," in *Proc. IEEE Conf. Decision and Control and European Control Conf.*, 2011, pp. 2195–2201.
- [24] S. Sundaram, M. Pajic, C. Hadjicostis, R. Mangharam, and G. J. Pappas, "The wireless control network: monitoring for malicious behavior," in *Proc. IEEE Conf. Decision and Control*, 2010.
- [25] H. Fawzi, P. Tabuada, and S. Diggavi, "Security for control systems under sensor and actuator attacks," in *Proc. IEEE Conf. Decision and Control*, 2012, pp. 3412–3417.

- [26] M. S. Chong, M. Wakaiki, and J. P. Hespanha, "Observability of linear systems under adversarial attacks," in *Proc. IEEE Amer. Control conf.*, 2015.
- [27] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, "Robustness of attack-resilient state estimators," in *Proc. ACM/IEEE Int. Conf. Cyber-Physical Systems*, Apr. 2014, pp. 163–174.
- [28] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *Proc. IEEE Conf. Decision and Control*, 2010, pp. 5967–5972.
- [29] Y. Mo and B. Sinopoli, "False data injection attacks in cyber physical systems," in *First Workshop on Secure Control Systems*, 2010.
- [30] R. Tibshirani, "Regression shrinkage and selection via the lasso," *J. the Royal Statistical Society. Series B (Methodological)*, pp. 267–288, 1996.
- [31] W. Rudin, *Principles of mathematical analysis*. McGraw-Hill New York, 1964, vol. 3.
- [32] B. Anderson and J. Moore, *Optimal Filtering*. Prentice Hall, 1979.